Grindrod Ship Management

a division of GRINDROD SHIPPING (SA)(PTY) LTD

MEMORANDUM

To: General Manager My Ref :

From**:** Brett McElligott Date: 6 June 2022

Good day Quentin

EMERGENCY RESPONSE CENTRE EXERCISE REPORT: 02 June 2022 @ 10h00 hrs

1. Purpose.

- To test company and vessel readiness should an emergency occur
- To test the ability of emergency response team to effectively work together to mitigate the effects of the incident
- To practice coordination between the different teams such as company emergency team and outside parties on a real time basis.
- To test the 24 hour emergency number and all communication equipment
- To test Grindrod Shipping response to the (simulated) media.
- To assess the effectiveness of implementation of contingency plan
- To understand and evaluate logistics requirement.
- To familiarize and to rehearse key personnel of their role during an emergency
- To identify the weakness / lapses (which can be improved later) in our system

2. Attendees

Rajesh Sharma	Incident Coordinator
Rajaraman Krisnamoorthy	Incident Manager
Rennie Govender	Technical Support
Mike Allen	Technical Support
Henry Dayo	Technical Support
Joey Baluyot	Technical Support
Zain Dhooma	IT Manager
Dereck Web	IT Representative
Warren King	Crewing Manager
Jaja Casas	Crewing Representative
Pat O'hara	Administrator – event recorder
Kerry Everett	SHEQ Representative – Sitrep recording
Tristan Hunt and Peter Priest	Secure Sphere IT Consultants
Brett McElligott	Facilitator

3. Exercise rule "Ransom – Cyber Security attack on IVS Hirono"

- SAFETY FIRST. All personnel on board shall be responsible for the safe Navigation and Operation during exercise. If an unsafe condition or operation is discovered, ensure to notify the team members. The Master to determine whether the situation can be corrected and if exercise should continue.

- Begin and end all telephone and radio conversations with the statement "**THIS IS A DRILL".** Ensure this statement is included on all email exercise documents.

- RECORDS - All documents and checklists exchanged by email used during the Exercise should be maintained. All details to be logged in the as an evidence of the Ship Shore Exercise.

- Some external communication – Flag state, P&I Club and Media (MTI) during this exercise shall be done only with the "role play" person. Port Authorities shall be communicated through agent or as required by agent.

- In the event of a REAL EMERGENCY THIS EXERCISE WILL BE TERMINATED

- All actions taken during the exercise, time, event, and description of activity (such as telephone call or personal contact) shall be recorded.

- ERC shall not be set up in the office in view of governmental restrictions and protection measures against Covid19 but emergency response/video conference shall be set up consisting of the response team members using MS Teams. The video conference shall be treated equivalent to the emergency response centre.

- Debriefing shall be held in ship/office after the exercise. During this debriefing, participants shall discuss the response and identify areas that were well handled, opportunities for improvement, and suggested action items.

- The Master shall follow-up this exercise with a debriefing and evaluation, involving all the exercise participants.

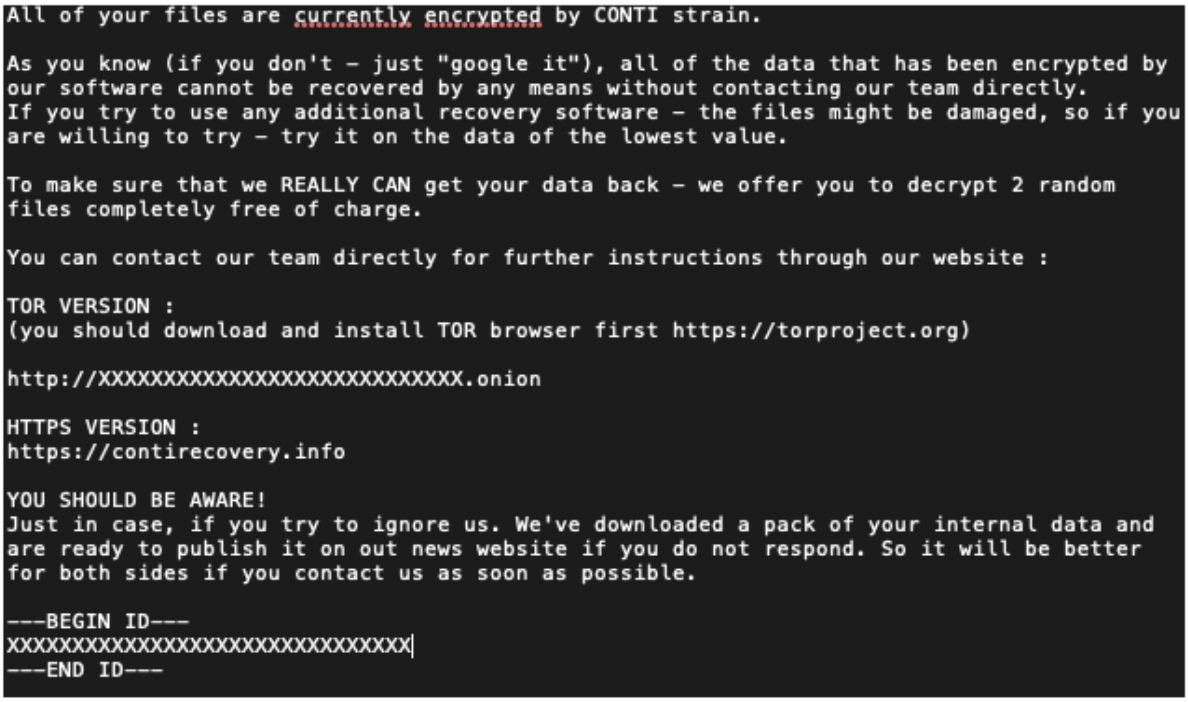
4. Scenario – Exercise "Ransom – Cyber Security attack on IVS Hirono"

a. The HIRONO is at anchorage or en-route to Tamatave Madagascar

SCENARIO STAGE 1

The Master of the vessel HIRONO was working on BASSNet HR Module updating onsigners and offsigners following a crew change in Richards Bay.

The following message appeared on the Master's Laptop:



Upon Investigation it appears that the Navigation Bridge PC has also been infected and the same sign appears on that pc.

Suspect that the server has also been compromised

EXERCISE 'Ransom' – HIRONO SCENARIO STAGE 2

Scenario Stage 2 – IMMEDIATE AFTERMATH (Only known to the Master)

It is discovered by a 3rd Party that the Conti Group has published on their News Site sample sets of data as proof of data exfiltration

5. Sequence of Events

	Appendix 1	
Date @ SGP Time	**Event Details**	**Action**
4.10pm	Master of Hirono phoned the Emergency number. The Master did not advise that it was a drill. Denver then just advised the Master to get in touch with the IT Department. Denver followed up with a call to Dereck to check the Master's laptop where the sign was seen on the laptop.	
4.25pm	The Master was then advised by BMM to phone the emergency number and advise Denver that it was a drill and that the ECR should convene. Denver was otherwise disposed therefore handed the emergency over to Rajaraman as first responder.	
4.30pm	Master called emergency Hotline informed IVS Hirono cyber-attack ransom message, Bridge and master's Laptop affected	
4.37pm	The virtual ERC convened including IT and Secure Spere Cyber Security Consultants	
4.38pm	Dereck Informed Master To remove the infected hardware from the infrastructure. to use Chief Engr Laptop instead	
4.39pm	Joey says to use a checklist no.43 - Cyber Security event.	
4.40pm	Rajesh informed Master not to interface ECDIS with any USB from the Nav Bridge PC which was infected.	
4.41pm	Media holding statement uploaded by Raja	
4.42pm	Class and flag informed	
4.43pm	Setting up teams on Chief laptop	
4.44pm	Zain says Triston from secure sphere (SS) joining the drill now	
4.45pm	SITREP being prepared	
4.46pm	Dereck briefing Triston from Secure sphere	
4.47pm	Screenshot of PC uploaded onto MS Teams	
4.48pm	Dereck and SS initiated scans on PC's and Vessel server.	
4.49pm	Checking on users' emails addresses to identify source of ransom demand	

4.52pm	Triston (SS) asking if any identified logins detected and has found an email	
4.56pm	Akshay talking to Master	
4.57pm	Joey to talk to Master and discover how this happened	
4.58pm	Raja briefed everyone again of their roles and recounting what had happened so far	
5.00pm	Rennie calling SM Brendon who had been missed out when assembling ECR.	
5.01pm	Mike to inform Hilton of the cyber-attack security breach	
5.02pm	initial report has been sent out to global emergencies email address.	
5.03pm	Tristian SS informed compromised while working on word document	
5.04pm	raja informed all communications on Chief computer on the Hirono	
5.05pm	Zain informed web access granted to master on chief computer	
5.06pm	Joey speaking to master	
5.06pm	Henry to inform commercial to contact him if unable to reach master via email	
5.07pm	Triatain SS asking to check with Master what he was doing	
5.07pm	Joey advised per Master working on HR module, outlook SharePoint, MS word is on when the attack occurred	
5.08pm	Hilton and Quentin updated	
5.09pm	Zain talking to Master, he has clarified an email received by Brett. To check with him if he is compromised.	
5.10pm	Zain briefing what BASSnet is and if this could be the issue.	
5.11pm	Brett's computer being checked now	
5.12pm	test message being sent out from ship	
5.13pm	Brendon to update Class and flag	
5.14pm	Crew details and personal data have been compromised	
5.15pm	counter measures explained by SS and system to be isolated and separated to still be able to continue work onboard.	

5.16pm	Brett's email account to be reset	
5.18pm	drop box is required for BASSnet therefore Dropbox is to be isolated.	
5.20pm	master to inform crew if any calls come in, that they should contact company media officer. And not to post anything on social media regards to this Top management, Warren King (crewing), Jan (HR) to be informed. Warren and Jaja confirmed the Crewing agencies were informed and are now handling the POPIA related issues as per our Manning agreement.	
5.23pm	Brett's computer to be investigated advised by SS	
5.25pm	Joey informing Sharon ting who is Company POPIA representative	
5.26pm	Brendon has updated Class and flag	
5.27pm	SITREP 2 sent out	
5.29pm	Media holding statement that crew info has been compromised	
5.30pm	Jaja and warren to inform manning agencies of situation	
5.32pm	Wi-Fi onboard has been disconnected interim	
5.34pm	drill ended	
5.35pm	debriefing	

6. Conclusion

All present expressed satisfaction with the drill. Minor issue was faced in setting up the video conference with the response team members. It was suggested that response team members should be pre-populated in the MS Team so that single click on the button is able to invite the required team members. It will be taken up with the IT Support.

7. Recommendations/Observations

	Feedback	**Whom**
1	The first responder holding the emergency line was indisposed and not near any of his laptop/iPad at the time. Any emergency call to the emergency number should be handed over to another member of the emergency team for follow up.	All to note
2	It is to be investigated whether when calling all SM's etc into a teams meeting the first responder could just send an invite to	IT/SHEQ

	Technical which all on technical will automatically be invited. It was noted that BG had not been called but he was the Vessel SM.	
3	It is imperative that the IM steps back and engages a holistic view of the incident, picking up information and reacting to the information. An example included making the CEO PC available for Teams meeting but only using the facility ½ hour later. The IT specialists continued to ask for information however these requests were ignored largely. The Master had vital information that was only relayed when the Master joined the teams meeting after ½ hour.	All to note
4	The IC was taking on too much instead of delegating to others in the drill. He is to have a more direct line with the Master of the vessel and to ensure this line (on MS Teams) is open ASAP.	All to note
5	Top management need to be informed as soon as personal information is breached, including Jeremy and Sharon. They will decide who to inform and when. IM unilaterally informed FLAG/Class without Directors consent. The Extent of the breach had not been established at time of informing external parties.	All to note
6	MTI to be notified but only after Senior Management had approved the release	All to note

Refer attached appendices

Appendix A – Drill Scenario and email sent to the vessel.
Appendix B – Expectations and outcomes of the Drill from Secure Sphere.
Appendix C – Email to the Vessel (Telecon twice prior to the drill with vessel)
Appendix D - Duties and Event Description
Appendix E - Initial report
Appendix F – Media Holding Statement
Appendix G - SITREP
Appendix H – PC rebuild procedure for specialist Software on affected PC's
Appendix I - Sundry records of Secure Sphere actions completed
Appendix J – Photo of Virtual ECR in Teams Meeting.

Kind Regards,

Brett McElligott
SHEQ Manager
Grindrod Ship Management, A Division Of Grindrod Shipping South Africa (Pty) Ltd
8th Floor, Grindrod House, 108 Margaret Mncadi Avenue (Victoria Embankment)
Durban 4001, South Africa
P O Box 3483, Durban, 4000, South Africa

☎: +27 (0)31 302 7964| : +27 (0)82 314 9983
✉ **brettm@grindrodshipping.com**

Appendix A

From: Brett McElligott - DURUNT
To: IVS HIRONO - MASTER (O365)
Subject: Drill 02/06/2022 Cyber Security- EXERCISE RANSOM
Date: Wednesday, 01 June 2022 20:08:19
Attachments: EXERCISE Ransom.docx
Conti message.PNG

Hi Mike

The Drill will commence at 10h00 SA time or earlier tomorrow. We are having our usual meeting at 08h00 then we will go on from there. I will give you a call tomorrow and we can set up before we go live.

The programs that were open on your laptop were the e-mail system and most importantly BASSNet HR Module and you were working with sign-on / signoff personnel.

It appears that BASSNet may have been compromised and that crew private information may have been leaked/stolen.

The NAV Bridge PC also has this message displayed.

The CONTI MESSAGE JPEG must be opened up and live on your screen for IT to View or take a WhatsApp and send it to the ECR.

Kind Regards,

Brett

Brett McElligott
SHEQ Manager
Grindrod Ship Management, A Division Of Grindrod Shipping South Africa (Pty) Ltd
8th Floor, Grindrod House, 108 Margaret Mncadi Avenue (Victoria Embankment)
Durban 4001, South Africa
P O Box 3483, Durban, 4000, South Africa
☎: +27 (0)31 302 7964| : +27 (0)82 314 9983
✉ **brettm@grindrodshipping.com**

EXERCISE "Ransom" - NOTIFICATION

Exercise "Ransom" is an exercise involving the Bulker HIRONO which is currently positioned in South Africa. The exercise is scheduled to take place on Thursday 2nd June 2022.

1. **PARTICIPANTS**
   MT HIRONO
   Grindrod Ship Management Durban – Ship Management/ERC Team.
   Secure Sphere Consulting – Cyber Security consultants
   Rennie and Akshey – Will be observers
   Brett McElligott is the facilitator.

   Hilton Stroebel and Quentin Foyle are not available to participate in the Drill.

   Note: The extent of involvement of Grindrod Ship Management satellite offices and external parties will be determined by the Grindrod Ship Management team as the need arises.

2. **GROUND RULES**
   a. **Safety is the first priority during the exercise.**
   b. In the event of a real emergency or the exercise becoming compromised the following message will be relayed to all parties **"STOP, STOP, STOP EXERCISE"**.
   c. Begin and end all calls, conversations, and e-mail with **"This is an exercise".**
   d. Simulated weather conditions will be used during the exercise.

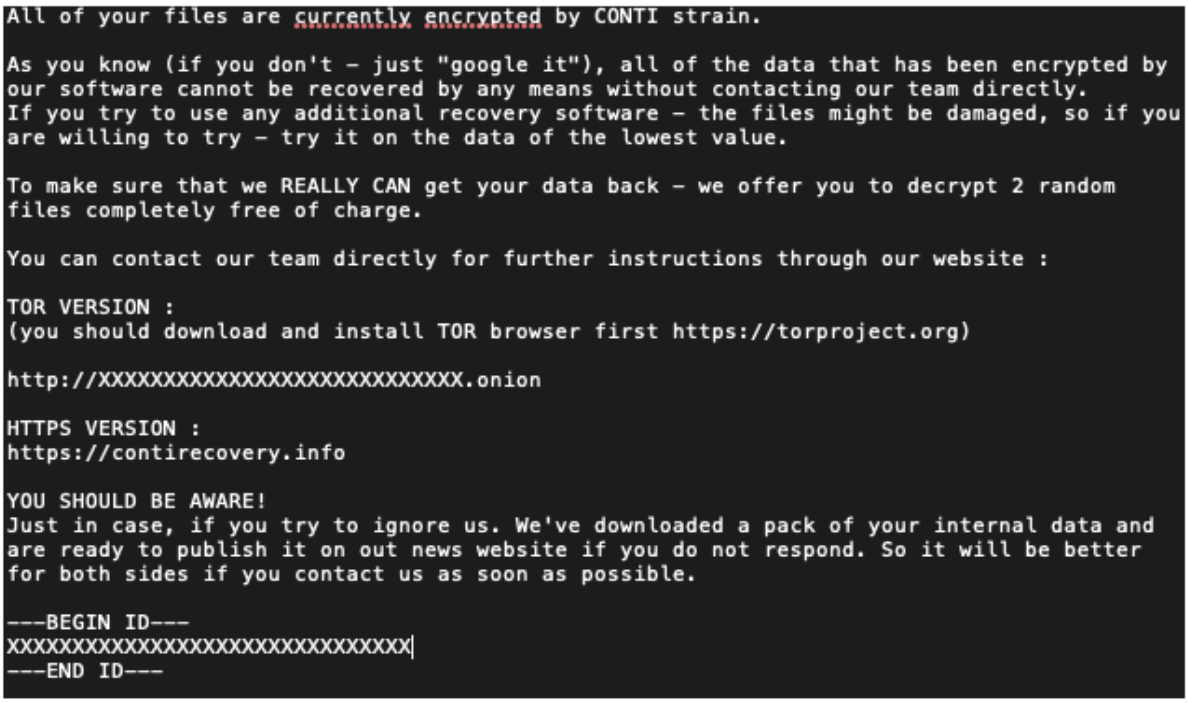
3. **OBJECTIVES OF THE EXERCISE**
   a. To test the ERC Team and vessels response to an un-announced exercise.
   b. To test ship/shore satellite communications.
   c. To provide the opportunity for the vessel and ERC team to practice handling an un-announced unfolding emergency and to test their response.
   d. To test media response.

4. **SCENARIO (Known to Master HIRONO)**
   a. The HIRONO is at anchorage or en-route to Tamatave Madagascar

EXERCISE 'Ransom' – HIRONO SCENARIO STAGE 1

The Master of the vessel HIRONO was working on BASSNet HR Module updating onsigners and offsigners following a crew change in Richards Bay.

The following message appeared on the Master's Laptop:



```
All of your files are currently encrypted by CONTI strain.

As you know (if you don't - just "google it"), all of the data that has been encrypted by
our software cannot be recovered by any means without contacting our team directly.
If you try to use any additional recovery software - the files might be damaged, so if you
are willing to try - try it on the data of the lowest value.

To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random
files completely free of charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :
(you should download and install TOR browser first https://torproject.org)

http://XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.onion

HTTPS VERSION :
https://contirecovery.info

YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded a pack of your internal data and
are ready to publish it on out news website if you do not respond. So it will be better
for both sides if you contact us as soon as possible.

---BEGIN ID---
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
---END ID---
```

Upon Investigation it appears that the Navigation Bridge PC has also been infected and the same sign appears on that pc.

Suspect that the server has also been compromised

EXERCISE 'Ransom' – HIRONO SCENARIO STAGE 2

Scenario Stage 2 – IMMEDIATE AFTERMATH (Only known to the Master)

- It is discovered by a 3rd Party that the Conti Group has published on their News Site sample sets of data as proof of data exfiltration

Appendix B

From: Jon Randall
To: Brett McElligott - DURUNT
Subject: Test Scenario option.
Date: Tuesday, 15 February 2022 09:12:59
Attachments: ssc_email_logo_49b369fc-17a5-4524-ae95-702c3fb65c38.png
1_sm_fb_54a3f780-aecc-4553-9f38-1e304c73bae1.png
1_sm_linkedin_62ce08ef-9203-4bc1-a2b9-094e51eb72c5.png
1_sm_twitter_976f6850-6446-408c-b9ef-a3e40e81bdb8.png
Grindrod Shipping - Test Scenario.docx

Hi Brett,

Please see attached doc.
Please read through it and let me know if this is something we can turn into a test case for GRD Shipping.
This is a very realistic scenario that has massive impact if not handled effectively.

Thanks,

Jon Randall
General Manager
Email: jon.randall@securesphere.co.za
Cell: 083 948 4941 • Phone: +27 31 100 0011
Website: www.securesphere.co.za

Grindrod Shipping – Test Scenario

Ransomware "fallout" – the worst-case scenario

What happened:

- There was an attack that took down a server
- The attack was successful, and the server was encrypted
- The attack was performed by the hacking group known as Conti
- A ransom note was left, and Grindrod Shipping chose not to pay
- The server was restored via a backup and put back into production

What should've happened:

- Full communication back to the business
- A risk & impact assessment done on the server
- Perform a forensics investigation
- Archive all security logs for any Regulator queries.
- Achieve a "clean bill of health"
- Notify the following parties:
    - The regulator
    - The affected customers
    - The authorities

What happens next:

- It is discovered by a 3rd Party that the Conti Group has published on their News Site sample sets of data as proof of data exfiltration
- Identify what the data is (download it) – if this cannot be confirmed then assume all data from the server is compromised.
- Identify what data was/is on the server that has been exfiltrated. (PII, IP, Financial, Client Info, other sensitive data)
- Clearly communicate the details and extent of the breach to key internal stakeholders.
- Prepare communication for internal staff
- Prepare communication for external contacts who's data has been compromised.
- Setup email address and contact number that external and internal people can contact to find out more information about their data that has been compromised.
- Engage PR and prepare press release content.
- A follow-up notice must be sent to the regulator, affected customers and the authorities
- Public and Media communications must be sent
- Extortion by a 3rd party is likely
- There will be an increase in attacks against Grindrod Shipping
- A clear and consistent message needs to be communicated to internal and external parties
- International impact must be assessed (GDPR, Nasdaq, etc.)
- Full RCA report is vital
- All logs are to be archived for the case

Notes:

BAS-NET is a possible target as it has a lot of POPI information

The exchange

Goal is to ensure the Grindrod Shipping is prepared and ready to cover ALL steps:

- Identification
- Remediation
- Mitigation
- Forensics
- Regulatory/Compliance requirements

Appendix C

From: Brett McElligott - DURUNT
To: IVS HIRONO - MASTER (O365)
Subject: Drill 02/06/2022 Cyber Security- EXERCISE RANSOM
Date: Wednesday, 01 June 2022 20:08:19
Attachments: EXERCISE Ransom.docx
Conti message.PNG

Hi Mike

The Drill will commence at 10h00 SA time or earlier tomorrow. We are having our usual meeting at 08h00 then we will go on from there. I will give you a call tomorrow and we can set up before we go live.

The programs that were open on your laptop were the e-mail system and most importantly BASSNet HR Module and you were working with sign-on / signoff personnel.

It appears that BASSNet may have been compromised and that crew private information may have been leaked/stolen.

The NAV Bridge PC also has this message displayed.

The CONTI MESSAGE JPEG must be opened up and live on your screen for IT to View or take a WhatsApp and send it to the ECR.

Kind Regards,

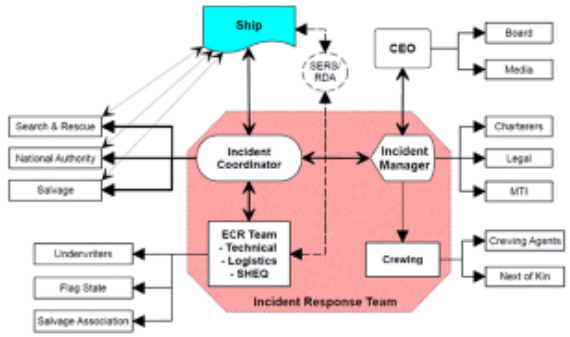
Brett

Brett McElligott
SHEQ Manager
Grindrod Ship Management, A Division Of Grindrod Shipping South Africa (Pty) Ltd
8th Floor, Grindrod House, 108 Margaret Mncadi Avenue (Victoria Embankment)
Durban 4001, South Africa
P O Box 3483, Durban, 4000, South Africa
☎: +27 (0)31 302 7964| : +27 (0)82 314 9983
✉ **brettm@grindrodshipping.com**

Appendix D

Duties and Event Description

Duties and event description



Function	Name of Person
Incident Manager	RAJARAMAN
Incident Coordinator	RAJESH
Technical Support	ZAIN / DERECK / CONSULTANT
Marine Support	MIKE ALLEN
Resource support	HENRY / JOEY
Logistics Support	NA
Event support	

Brett Not Available - he will be facilitating the drill

Hilton and Quentin will not be participating however should be notified as and when things develop as per our Emergency response procedure.

Entity to be notified	Complete	Contact Numbers
CHAIRMAN BOARD	YES	
OWNERS	YES	
IVS OPERATORS	YES	
CHARTERERS	YES	
H&M	NA	
P&I – UK CLUB	NA	
MEDIA MONITORING	YES	
COMPANY DOCTOR	NA	
AGENTS	NA	
NATIONAL AUTHORITY (AS PER SOPEP CONTACT LIST)	NA	
USCG	NA	
DI	NA	
MMCC	NA	
FLAG STATE	YES	
CLASS (NK /ABS/DNV)	YES	
CREW FAMILY BY CREWING DEPT.	NA	
ARMED GUARD COMPANY	NA	
K&R/INSURANCE COMPANY	NA	
PORT AUTHORITIES	NA	
SALVAGE	NA	
LAWYERS	NA	
OSRO	NA	

Re Initial Report

All Emails are to be sent to the following address: globalerc@grindrodshipping.com

Initial Report

All Emails are to be sent to the following address: globalerc@grindrodshipping.com

Emergency Contact No: **+65 66321380 / +27 31 302 7205**

Emergency Response Initial Report - DRILL DRILL DRILL

Ship's Name	IVS HIRONO
IMO number	9726229
• **Date / Time of call from vessel**:	02 JUNE / 1600
Who contacted the Office:	MIKE MELLY
• **Description of Incident**:	BRIDGE AND LAPTOP COMPUTER GOT INFECTED / RANSOM WARE
• **Location of incident on board:**	BRIDGE AND MASTERS CABIN
• **Any injuries / casualties**:	NIL
• **Damages**:	RANSOM WARE
• **Date / Time of incident on board:**	2nd May/1600 Hrs
• **Ship's position**:	At Sea 21-36.12S, 048-48.1 E
• **Course**	016
• **Speed**	11.6
• **Cargo On-board and quantity**:	Coal , 57550 MT
• **Bunker quantity on board**:	707 FO, 115 LSMGO
• **Any Oil Spill**:	NIL
• **Approx Quantity spilt over board**:	NIL
• **Next Port and distance**	bound to Tamatave, ETA 03rd May/0900 hrs

Weather conditions:	
• **Wind:**	
• **Direction :**	SSE
• **Speed (Beaufort):**	24 knots
• **Sea:**	
• **Direction**	
• **Height (m)**	2.0m

Reminder: Master/Office to follow the relevant contingency plan

Event Media Holding Statement Example

Thursday, 2 June 2022 4:30 pm

All Emails are to be sent to the following address: globalerc@grindrodshipping.com

Media Holding Statement

DRILL DRILL DRILL

To be released once approved by Grindrod Shipping Senior Management

- ***IVS HIRONO***
- ***CYBER SECURITY ATTACK***

Further information will be provided as it becomes available.

For any media enquiries, please contact MTI International.

MTI SGM (local Correspondent):

MTI London: Pat Adamson + 44 7836766947

www.mtinetwork.com

Appendix G

SITREP

All Emails are to be sent to the following address: globalerc@grindrodshipping.com

FOLLOW UP SITUATION REPORT

Ship Name:	IVS HIRONO
SITREP No:	01
Date and Time (UTC) of situation report:	02 June /
Summary / Update of the incident	
Update of the incident	Bridge and Laptop infected - both laptops removed from network. Captain using Chief Engineer computer Users e-mails addresses checked to identify source of ransom Virus came through word doc attached to e-mail Captain confirmed he was working on HR Module, Sharepoint, and Word. Captain mentioned he received an e-mail with attachment from Brett McElligott - his computer will also be checked. Crew details have been compromised via Bassnet HR Module.
Information received from:	Captain Melly
Number/Details of Casualties:	Nil
Damage:	Bridge and Laptop computer infected with Conti ransomware
Any external assistance required:	Secure Sphere
Authorities Involved:	Class & Flag informed
Emergency Services Involved:	NA
Response Services Involved:	NA
Company Emergency Response Activities:	ACTIVATED
Press Media Coverage	na
Press Response:	na
Report Sheet Issued By:	
Name:	Kerry Everett
Title:	SHEQ Representative
Contact Details:	031 3027911

FOLLOW UP SITUATION REPORT

Ship Name:	IVS Hirono
SITREP No:	02
Date and Time (UTC) of situation report:	02 June 2022 / 17:22
Summary / Update of the incident	
Update of the incident	Crew detail have been compromised Dropbox to be taken offline Server needs to be isolated and reset Brett McElligott's pc to be isolated and reset POPI act has been compromised
Information received from:	Captain Melly
Number/Details of Casualties:	Nil
Damage:	Bridge and Laptop computer infected with Conti ransomware
Any external assistance required:	Secure Sphere
Authorities Involved:	Class & Flag Informed
Emergency Services Involved:	Nil
Response Services Involved:	Nil
Company Emergency Response Activities:	Activated
Press Media Coverage	Nil
Press Response:	Nil
Report Sheet Issued By:	
Name:	Kerry Everett
Title:	SHEQ Representative
Contact Details:	031 3027911

GRINDROD SHIPPING

FOLLOW UP SITUATION REPORT

Ship Name:	IVS Hirono
SITREP No:	03
Date and Time (UTC) of situation report:	02 June 2022 /
Summary / Update of the incident	
Update of the incident	Media holding statement sent WIFI to be disconnected on the vessel
Information received from:	Captain Melly
Number/Details of Casualties:	Nil

Damage:	Bridge and Laptop computer infected with Conti ransomware
Any external assistance required:	Secure Sphere
Authorities Involved:	Class & Flag Informed
Emergency Services Involved:	Nil
Response Services Involved:	Nil
Company Emergency Response Activities:	Activated
Press Media Coverage	MTI
Press Response:	Nil
Report Sheet Issued By:	
Name:	Kerry Everett
Title:	SHEQ Representative
Contact Details:	031 3027911

GRINDROD SHIPPING

FOLLOW UP SITUATION REPORT

Ship Name:	
SITREP No:	
Date and Time (UTC) of situation report:	
Summary / Update of the incident	
Update of the incident	
Information received from:	
Number/Details of Casualties:	
Damage:	
Any external assistance required:	
Authorities Involved:	
Emergency Services Involved:	
Response Services Involved:	
Company Emergency Response Activities:	
Press Media Coverage	
Press Response:	
Report Sheet Issued By:	
Name:	

From: Rajaraman Krishnamoorthy - GSM SG
To: Zain Dhooma - GSH DBN; Brett McElligott - DURUNT
Cc: Akshay Ramriky - GSH DBN; Rajesh Sharma - GSH SG
Subject: RE: HIRONO
Date: Monday, 06 June 2022 03:50:43

Hi Zain

Vessel has ECHART DVD onboard.

We can use this for downloading the program on the computer.

Updates can be done via internat.

Brgds
Raja

From: Zain Dhooma - GSH DBN <zaind@grindrodshipping.com>
Sent: Thursday, 2 June 2022 7:46 pm
To: Rajaraman Krishnamoorthy - GSM SG <RajaramanK@grindrodshipman.com>; Brett McElligott - DURUNT <BrettM@grindrodshipping.com>
Cc: Akshay Ramriky - GSH DBN <AkshayR@grinship.global>
Subject: Re: HIRONO

Hi

Hi

In a case of an emergency we need to work out how we get these applications working online with only internet access at our disposal.

ADP
eNP
ChartBrowswer
Master outlook – Online with Office365
SharePoint - Online with Office365
SHEQ – Online with Appstage

Can we check with the providers how we go about accessing the data on the first 3 to ensure that we have complete redundancy.

Thanks
Zain

From: Akshay Ramriky - GSH DBN <AkshayR@grinship.global>
Date: Thursday, 02 June 2022 at 10:45
To: Zain Dhooma <zaind@grindrodshipping.com>, Rajaraman Krishnamoorthy - GSM SG <RajaramanK@grindrodshipman.com>, Brett McElligott <BrettM@grindrodshipping.com>
Subject: HIRONO

Hi All,

List of software to restore backup.

ADP
eNP
ChartBrowswer
Master outlook
SharePoint
SHEQ

Thanks

Akshay Ramriky
Marine IT Technician
Grindrod Shipping South Africa (Pty) Ltd
8th Floor, Grindrod House, 108 Margaret Mncadi Avenue (Victoria Embankment)
Durban 4001, South Africa
P O Box 3483, Durban, 4000, South Africa
☎ *: +27 31 302 1808 office|* 📞*: +27 60 9766 923 mobile*
✉ ***Akshayr@grindrodshipping.com***

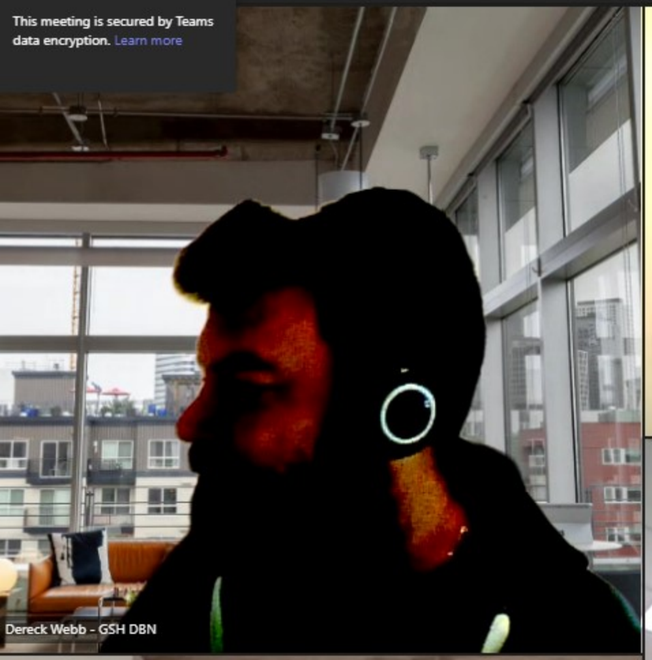
Email Legal Notice - http://www.grinshipping.com/Content/EmailLegalNotice

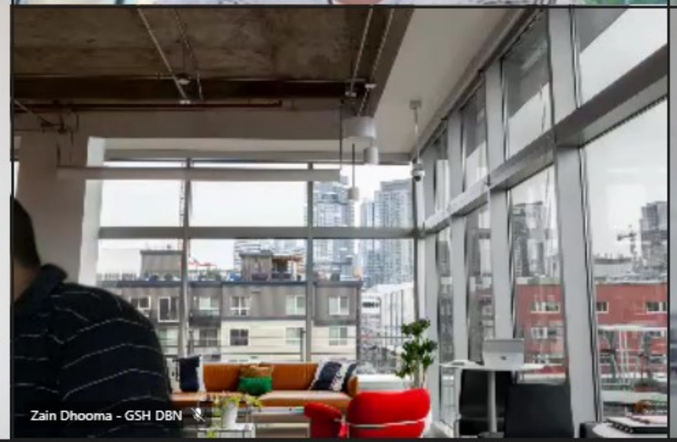
CYBER SECURITY - DRILL DRILL DRILL

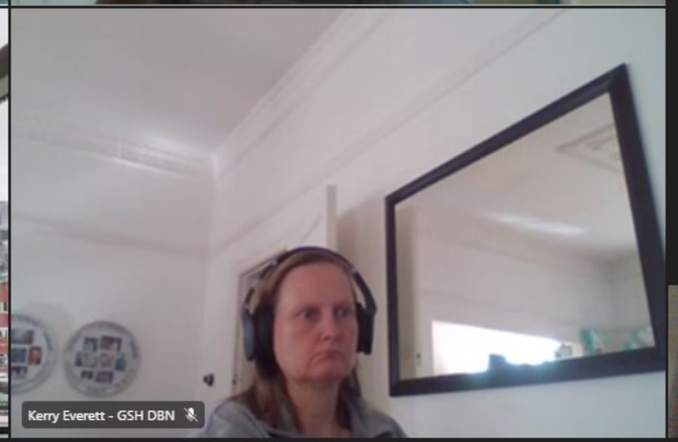
15:53

This meeting is secured by Teams data encryption. Learn more

People | Chat | Reactions | Rooms | Apps | More | Camera | Mic | Share | Leave







AR Akshay Ra...

IM IVS HIRON...

TH Tristan Hunt

MA Mike Allen -...

PP Peter Priest

Meeting chat

Rajaraman Krishnamoorthy - GSM SG joined the conversation.

Today

Rajaraman Krishnamoorthy - GSM SG named the meeting to CYBER SECURITY - DRILL DRILL DRILL.

Joey Baluyot - GSM SG and 10 others were invited to the meeting.

4:30 pm Meeting started

Kerry Everett - GSH DBN was invited to the meeting.

Patricia O' Hara - GSM SG 4:42 pm
zain who is that again

Zain Dhooma - GSH DBN

IVS HIRONO Master (Guest) was invited to the meeting.

Tristan Hunt was invited to the meeting.

Peter Priest was invited to the meeting.

Patricia O' Hara - GSM SG 4:46 pm
peter priest is in

Dereck Webb - GSH DBN 4:46 pm

Type a new message